CLAIMS

1. A signal processing system having a reproducing apparatus for reading information from a recording medium having information unique thereto and an information processing apparatus for mutually authenticating and connecting the reproducing apparatus through a transferring portion,

wherein the reproducing apparatus comprises:

final encryption key generating means for generating a content information encryption key in accordance with intermediate key information;

a first transmitting portion for transmitting the intermediate key information to the information processing apparatus through the transferring portion; and

a second transmitting portion for transmitting the content information encryption key to the information processing apparatus through the transferring portion, and

wherein the information processing apparatus comprises:

a content information encrypting portion for encrypting content information using the content information encryption key;

an intermediate key information encrypting portion for encrypting the intermediate key information using key information unique to the recording medium,

the key information being generated in accordance with information unique to the recording medium; and

a recording portion for recording the encrypted content information and the encrypted intermediate key information to the recording medium.

2. The signal processing system as set forth in claim 1,

wherein the reproducing apparatus further comprises a random number generating portion for generating a random number, and

wherein the intermediate key information is a random number generated by the random number generating portion.

3. A recording method of a reproducing apparatus and an information processing apparatus for recording information to a recording medium, the reproducing apparatus being configured to read information from the recording medium having information unique thereto and the information processing apparatus being configured to mutually authenticate and connect the reproducing apparatus through a transferring portion, the recording method comprising the steps of:

causing the reproducing apparatus to generate a content information encryption key in accordance with intermediate key information;

causing the reproducing apparatus to transmit the intermediate key information to the information

processing apparatus through the transferring portion;

causing the reproducing apparatus to transmit the content information encryption key to the information processing apparatus through the transferring portion;

causing the information processing apparatus to encrypt content information using the content information encryption key;

causing the information processing apparatus to encrypt the intermediate key information using key information unique to the recording medium, the key information being generated in accordance with information unique to the recording medium; and

causing the information processing apparatus to record the encrypted content information and the encrypted intermediate key information to the recording medium.

4. The recording method as set forth in claim 3, further comprising the step of:

causing the reproducing apparatus to generate a random number,

wherein the intermediate key information is a random number generated at the random number generating step.

5. A program of a reproducing apparatus and an information processing apparatus for recording information to a recording medium, the reproducing

apparatus being configured to read information from the recording medium having information unique thereto and the information processing apparatus being configured to mutually authenticate and connect the reproducing apparatus through a transferring portion, the program comprising the steps of:

causing the reproducing apparatus to generate a content information encryption key in accordance with intermediate key information;

causing the reproducing apparatus to transmit the intermediate key information to the information processing apparatus through the transferring portion;

causing the reproducing apparatus to transmit the content information encryption key to the information processing apparatus through the transferring portion;

causing the information processing apparatus to encrypt content information using the content information encryption key;

causing the information processing apparatus to encrypt the intermediate key information using key information unique to the recording medium, the key information being generated in accordance with information unique to the recording medium; and

causing the information processing apparatus to record the encrypted content information and the encrypted intermediate key information to the recording

medium.

6. The program as set forth in claim 5, further comprising the step of:

causing the reproducing apparatus to generate a random number,

wherein the intermediate key information is a random number generated at the random number generating step.

7. A recording medium for storing a program of a reproducing apparatus and an information processing apparatus for recording information to a recording medium, the reproducing apparatus being configured to read information from the recording medium having information unique thereto and the information processing apparatus being configured to mutually authenticate and connect the reproducing apparatus through a transferring portion, the program comprising the steps of:

causing the reproducing apparatus to generate a content information encryption key in accordance with intermediate key information;

causing the reproducing apparatus to transmit the intermediate key information to the information processing apparatus through the transferring portion;

causing the reproducing apparatus to transmit the content information encryption key to the information processing apparatus through the

transferring portion;

causing the information processing apparatus to encrypt content information using the content information encryption key;

causing the information processing apparatus to encrypt the intermediate key information using key information unique to the recording medium, the key information being generated in accordance with information unique to the recording medium; and

causing the information processing apparatus to record the encrypted content information and the encrypted intermediate key information to the recording medium.

8. The recording medium as set forth in claim 7, further comprising the step of:

causing the reproducing apparatus to generate a random number,

wherein the intermediate key information is a random number generated at the random number generating step.

9. A reproducing apparatus, connected to an information processing apparatus through a transferring portion, for reading information from a recording medium having information unique thereto, the reproducing apparatus comprising:

final encryption key generating means for generating a content information encryption key in

accordance with intermediate key information;

a first transmitting portion for transmitting the intermediate key information to the information processing apparatus through the transferring portion;

a second transmitting portion for transmitting the content information encryption key to the information processing apparatus through the transferring portion,

wherein the reproducing apparatus is mutually authenticated with the information processing apparatus and connected thereto, the information processing apparatus comprising a content information encrypting portion for encrypting content information using the content information encryption key; an intermediate key information encrypting portion for encrypting the intermediate key information using key information unique to the recording medium, the key information being generated in accordance with information unique to the recording medium; and a recording portion for recording the encrypted content information and the encrypted intermediate key information to the recording medium.

10. The reproducing apparatus as set forth in claim 9, further comprising:

a random number generating portion for generating a random number, and

wherein the intermediate key information is a

random number generated by the random number generating portion.

11. An information processing apparatus connected to a reproducing apparatus through a transferring portion, the reproducing apparatus being configured to read information from a recording medium having information unique thereto, the information processing apparatus being mutually authenticated with the reproducing apparatus and connected thereto through the transferring portion, the reproducing apparatus comprising final encryption key generating means for generating a content information encryption key in accordance with intermediate key information; a first transmitting portion for transmitting the intermediate key information to the information processing apparatus through the transferring portion; and a second transmitting portion for transmitting the content information encryption key to the information processing apparatus through the transferring portion, the information processing apparatus comprising:

a content information encrypting portion for encrypting content information using the content information encryption key;

an intermediate key information encrypting portion for encrypting the intermediate key information using key information unique to the recording medium, the key information being generated in accordance with

information unique to the recording medium; and

a recording portion for recording the encrypted content information and the encrypted intermediate key information to the recording medium.

12. The information processing apparatus as set forth in claim 11,

wherein the reproducing apparatus further comprises a random number generating portion for generating a random number, and

wherein the intermediate key information is a random number generated by the random number generating portion.

13. A reproducing apparatus, comprising:

at least one of a recording portion for recording encrypted data to a recording medium on which first information for invalidating an illegal electronic device, second information that differs in each content, third information definable for each encrypted unit, and identification data that differs in each stamper are pre-recorded and a reproducing portion for reproducing encrypted data recorded on the recording medium;

a storing portion for storing fourth information unique to a valid electronic device or application software;

a revoking processing portion for determining whether or not the forth information is information

unique to a valid electronic device or application software using the first information and the fourth information;

a calculating portion for obtaining intermediate key information unique to each recording medium using the first information, the fourth information, the second information, and the identification data when the determined result of the revoking processing portion represents that the fourth information is information unique to a valid electronic device or application software; and

a transmitting portion for transmitting the intermediate key information to the final encryption key generating portion of an information processing apparatus through a transferring portion.

14. The recording and reproducing apparatus as set forth in claim 13, further comprising:

an authenticating portion for mutually authenticating a data processing apparatus for at least encrypting data or decrypting encrypted data using a key generated in accordance with the intermediate key information; and

an intermediate key information encrypting portion for encrypting the intermediate key information using a session key generated when the authentication has been successfully performed and transmitting the encrypted intermediate key information to the data

processing apparatus.

15. A data processing apparatus, comprising:

an authenticating portion for authenticating a recording and reproducing apparatus, the recording and reproducing apparatus having fourth information unique to a valid electronic device or application software, for at least recording encrypted data to a recording medium on which first information for invalidating an illegal electronic device, second information that differs in each content, third information definable for each encrypted unit, and identification data that differs in each stamper are pre-recorded or reproducing encrypted data recorded on the recording medium;

a key information decrypting portion for receiving the first information, the fourth information, and intermediate key information from the recording and reproducing apparatus and decrypting the intermediate key information, the first information and the forth information having been encrypted using a session key generated when the authentication has been successfully performed, the intermediate key information being unique to each recording medium and generated using the second information and the identification data;

a final encryption key generating portion for generating a final encryption key using the third information received from the recording and reproducing

apparatus and the decrypted intermediate key information; and

an encrypting and decrypting portion for at least encrypting data using the final encryption key or decrypting data using the final encryption key.